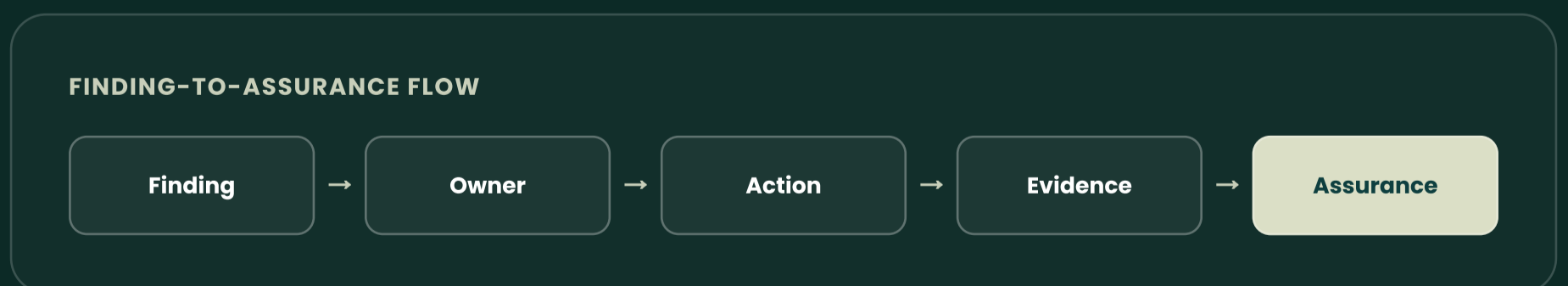


# Finding-to-Assurance Flow

How industrial organisations turn OT cyber findings into owned actions, verified evidence and assurance-ready outcomes



# 01 Executive Summary

Most OT cyber assessments do their job. They identify gaps, expose control weaknesses and create a record of risk. But assessment output is not assurance.

A finding does not reduce risk until it becomes owned work, completed action, verified evidence and a governed risk outcome.

■ **Assessment is observation. Assurance is governed execution.**

## Why findings stall

Assessment findings often stop short of assurance.

## Where gaps appear

Ownership, evidence and verification can break down.

## What assurance needs

Findings need owner, action, evidence and risk outcome.

## How to act

Test the model with one controlled example.

## 02 Assessment Is Not Assurance

Many organisations treat assessment completion as progress. It is progress, but it is not proof that risk is being reduced.

Assessments create visibility. They do not assign owners by themselves. They do not complete actions. They do not verify evidence. They do not decide whether residual risk is acceptable.

### ASSESSMENT-TO-ASSURANCE GAP



#### The issue

Findings often move across OT, IT, engineering, operations and suppliers.

#### The risk

Ownership blurs, evidence scatters and decisions become unclear.

## 03 What Assurance Really Requires

Assessment outputs are useful, but they need to be converted into controlled execution.

Common View	What Assurance Requires
A completed assessment means risk is under control.	Each finding needs an owner, action, evidence trail and risk outcome.
A risk heatmap shows what to fix.	Risk treatment needs a decision, owner and evidence path.
A roadmap creates control.	Actions must be assigned, delivered, evidenced and verified.
Evidence documents prove assurance.	Evidence must be reviewed against the finding and control objective.
Closure means completion.	Closure must be linked to verification and residual-risk decision.

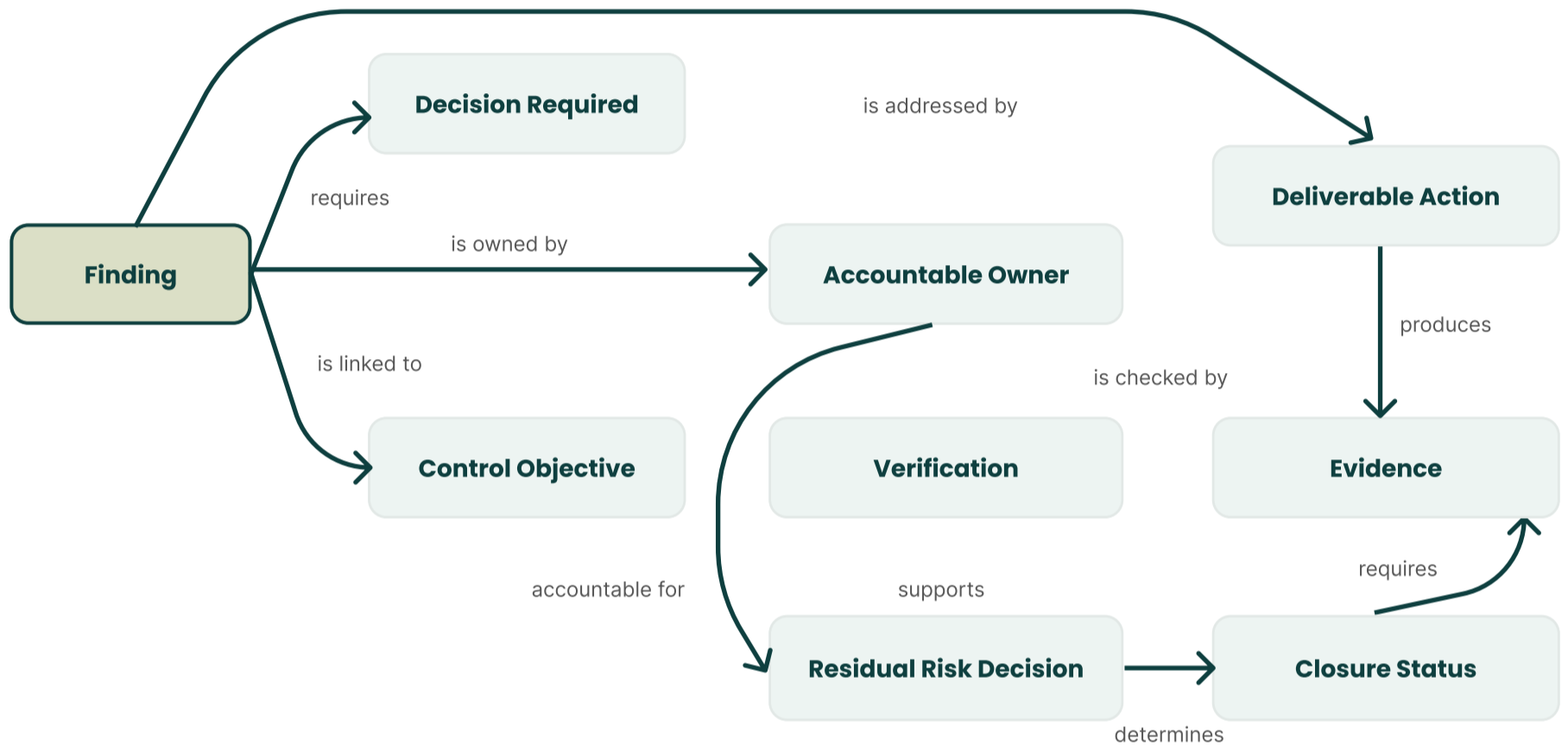
■ Findings do not reduce risk until they are owned, actioned and evidenced.

## 04 Finding Breakdown Ontology

A finding becomes assurance-ready only when the required objects and relationships are controlled.

The ontology below shows the core objects and how they connect.

### FINDING-CONTROL ONTOLOGY



### COMMON BREAKDOWN POINTS



- Ownership unclear
- Evidence scattered
- Verification weak
- Decision missing

## 05 What Assessment Outputs Need to Become Assurance

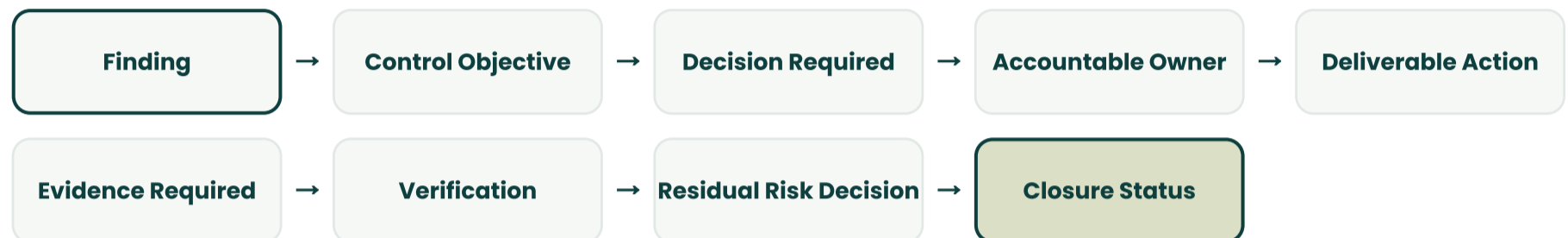
Assessment outputs are not the problem. The gap appears when they are not connected to ownership, action, evidence and decision-making.

Assessment Output	What It Shows	What Assurance Needs
Finding	A gap has been recorded.	Named owner, action and verified evidence.
Risk heatmap	Risk has been ranked.	Treatment decision, owner and evidence path.
Framework mapping	Alignment has been shown.	Obligation owner, action, evidence and verification.
Remediation roadmap	Planned work has been listed.	Owned delivery, due dates and verified evidence.
Maturity score	Current position has been measured.	Verified control status and evidence chain.
Exception	A deviation has been recorded.	Approved decision, owner and residual-risk outcome.
Evidence document	Proof may exist.	Evidence review, verification and decision trail.

## 06 The Finding-to-Assurance Flow

The better model is to control each finding through decision, owner, action, evidence, verification and assurance.

### FINDING-TO-ASSURANCE FLOW



This flow turns a finding from a static record into an executable assurance path. It makes clear:

- what needs to be controlled
- who owns the outcome
- what action is required
- what evidence is acceptable
- who verifies the outcome
- what residual risk remains
- whether closure is justified

## 07 The Nine Control Points

Each finding should pass through nine control points. The control questions make the assurance path explicit.

### 01 Finding

What exactly needs to be addressed?

### 02 Control Objective

What control outcome must be achieved?

### 03 Decision Required

What decision is required before work can proceed or close?

### 04 Accountable Owner

Who owns the risk outcome?

### 05 Deliverable Action

What work must be completed?

### 06 Evidence Required

What evidence will prove the action was completed?

### 07 Verification

Who verifies that the evidence is acceptable?

### 08 Residual Risk

What risk remains, and who accepts it?

### 09 Closure Status

Is closure justified and defensible?

## 08 The Assurance Gap Looks Different for Each Role

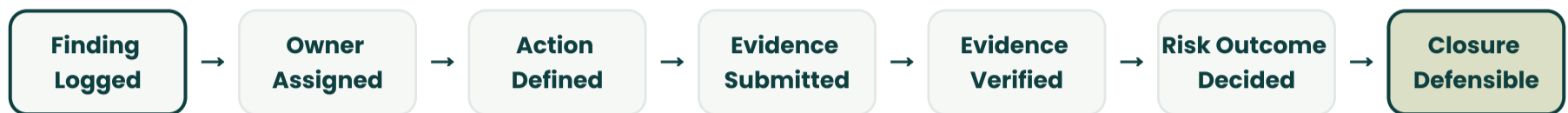
When findings are not controlled, each role carries a different part of the risk.

Role	What They Experience	What They Need
Delivery teams	Findings do not become clear work.	Named owners, due actions, deadlines and evidence requirements.
Assurance and compliance leads	Framework alignment does not prove control assurance.	Traceable chain from obligation to owner, action, evidence, exception and status.
Executives	Assessment completion does not prove risk is reducing.	Clear visibility of delivery risk, evidence gaps and accountability exposure.
Auditors	Evidence is available but not clearly linked to decisions.	Defensible evidence chains and decision records.
Suppliers and contractors	Evidence requests arrive late or inconsistently.	Clear evidence expectations and controlled submission paths.

## 09 From Finding to Assurance-Ready Status

A finding only becomes assurance-ready when it has moved through a controlled path.

### ASSURANCE-READY PATH



This does not mean every finding must be closed immediately. It means each finding must have:

- a known state
- a named owner
- a defined next action
- a clear evidence position
- a decision path

■ That is what turns assessment output into managed assurance.

## 10 How to Use the Flow

Start with one controlled example: a live assessment finding, project finding or supplier delivery issue. Do not use sensitive network, asset, vulnerability or customer data. The flow works with the structure of the finding, not the confidential detail.

Check	Question
Finding	Is the finding clear enough to act on?
Control objective	Is the intended control outcome defined?
Decision	Is a treatment, exception or acceptance decision required?
Owner	Is there a named accountable owner?
Action	Is the required work clear?
Evidence	Is the required evidence defined?
Verification	Is there a verification step and reviewer?
Residual risk	Is the remaining risk owned and accepted?
Closure	Is closure supported by evidence and decision trail?

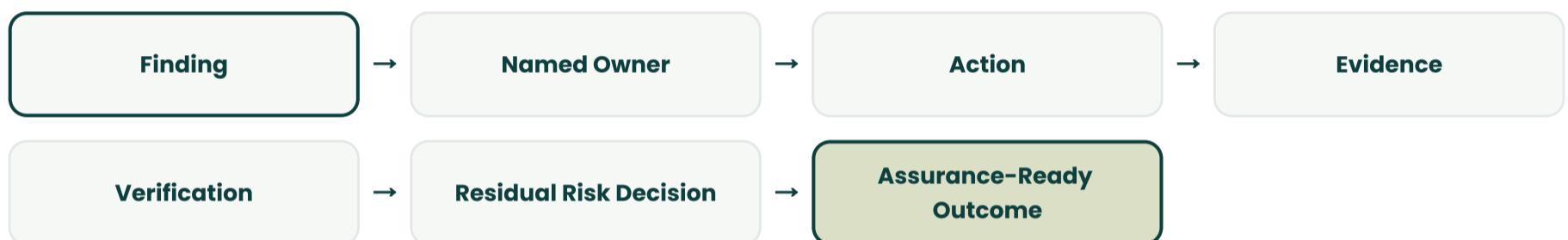
## 11 The Better Way: From Assessment Output to Assurance

Once the gap is visible, the better model becomes clear. Assessment output must be converted into controlled execution.

### BEFORE: ASSESSMENT OUTPUT WITHOUT EXECUTION CONTROL



### AFTER: FINDING-TO-ASSURANCE FLOW



■ The before state records the problem. The after state controls the outcome.

## 12 What the Pattern Reveals

Testing one finding can show whether the problem is isolated or repeated.

### PATTERN RECOGNITION



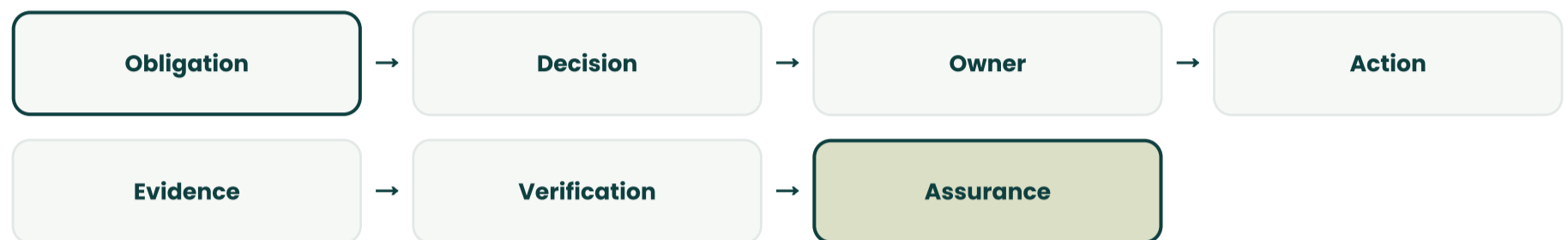
Repeated gaps usually expose one or more of the following:

- unclear accountability
- weak evidence lifecycle
- manual assurance effort
- poor supplier interface control
- weak residual-risk governance
- incomplete closure discipline
- board reporting based on trust rather than proof

## 13 Corgenta Execution Control Model

Corgenta turns assessment outputs into controlled execution. It helps industrial teams move from findings and obligations to named owners, delivered actions, verified evidence and governed risk outcomes.

### CORGENTA EXECUTION CONTROL MODEL



With Corgenta, findings do not sit as disconnected records. They become part of a governed execution model where ownership, evidence, decisions and assurance status remain connected.

- keep findings connected to risk and control outcomes
- make ownership explicit
- define evidence before closure
- verify evidence as work is delivered
- govern residual-risk decisions
- make assurance defensible

## 14 If This Resonates With You, Then Act on It

If the flow exposes weak ownership, scattered evidence or manual assurance effort, the next step is to test three findings in a Cyber Delivery Gap Review.

A structured review helps make the issue visible earlier. It can help your organisation:

- identify where findings lose ownership
- expose where evidence becomes scattered or unverifiable
- understand where supplier dependency affects assurance
- identify where residual-risk decisions are missing or weak
- clarify where closure status is not defensible
- prioritise improvements based on risk and business value

### FROM RECOGNITION TO ACTION



## 15 Request a Cyber Delivery Gap Review

A Cyber Delivery Gap Review uses three findings to expose where ownership, action, evidence, supplier dependency, verification, residual risk or closure breaks down.

### Review examines

Finding ownership, decision requirements, action traceability and evidence lifecycle.

### Supplier interface

Supplier and contractor dependencies, verification route and closure discipline.

### Outcome

Practical observations and prioritised recommendations.

### Data position

No sensitive project, network, asset, vulnerability or customer data required.

### REVIEW OUTCOME



## 16 About Corgenta

Corgenta is an OT Governance, Risk and Compliance execution platform.

It helps organisations manage cybersecurity delivery across requirements, controls, projects, evidence, governance and compliance.

Corgenta is designed for industrial environments where assurance depends on controlled execution across multiple teams, suppliers and delivery organisations.

### CORGENTA PLATFORM SPINE



- **Risk is reduced when findings become owned actions, verified evidence and governed outcomes.**

The practical question is whether your findings are becoming assurance, or whether they are becoming another source of hidden delivery friction.

**Next step: Request a Cyber Delivery Gap Review**